IN THE CLAIMS

75. (Currently Amended) A method of authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communication channel, said method including the steps of:

generating a first challenge signal of minimum duration T, where T is a fixed time interval and is larger than the channel transmission and processing delay;

generating a random number x, computing g^x modulo p, where g and p are numbers, deriving a key k_A from g^x modulo p, encrypting said first challenge signal with the key k_A and a symmetric key cryptosystem to provide a first ciphertext, and sending athe first ciphertext to said remote party;

receiving a second ciphertext from said remote party~~,~~;

sending g^x modulo p to said remote party~~,~~ and starting a clock;

receiving ~~a third ciphertext and~~ g^y modulo p from said remote party;

receiving a third ciphertext from said remote party, stopping the clock after receiving the third ciphertext~~,~~ and computing an elapsed time interval of said clock;

deriving a key k_B from received g^y modulo p~~, computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p~~, decrypting said second ciphertext with the key k_B to recover a second challenge signal from said remote party~~;~~

computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p;

decrypting said third ciphertext with the key k_{AB} to recover a first response signal from said remote party;

verifying that said elapsed time of the clock is within a predetermined interval (TL_A, TU_A), where TL_A and TU_A are positive numbers;

verifying that said second challenge signal is produced by said remote party;

producing a second response signal of minimum duration T, encrypting said second response signal with the key k_{AB} to provide a fourth ciphertext and sending athe fourth ciphertext to said remote party;

verifying that said first response signal is a response produced by said remote party to said first challenge signal; and

after verifying that said second challenge signal and that said first response signal are produced by said remote party and that said elapsed time is within the predetermined interval, ~~generating~~ using a key k from g^{xy} modulo p for secure communications with said remote party.

76. (Currently Amended) The method according to claim 75, wherein said challenge signals and response signals represent biometrics characteristics ~~(such as voice signals)~~ of the ~~producing~~ authenticating and remote parties.

77. (Currently Amended) The method according to claim 75, wherein verification of said first response signal and said second challenge signal from said remote party ~~is~~ are based on familiarity ~~of~~ with the remote party's biometrics characteristics. ~~Encryption of said challenge and response signals is performed using a cryptographic commitment function.~~

78. (Previously Presented) The method according to claim 75, where TL_A is $t_1 + t_2$ and TU_A is $t_1 + t_2 + T$, with t_1 being the duration of said first challenge signal and t_2 being the duration of said first response signal.

79. (Currently Amended) An apparatus for authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communication channel, said apparatus including:

means for generating a first challenge signal of minimum duration T, where T is a fixed time interval, and ~~it~~ is larger than the channel transmission and processing delay;

means for generating a random number x, computing g^x modulo p, where g and p are numbers, deriving a key k_A from g^x modulo p, encrypting said first challenge signal with the key k_A and a symmetric key cryptosystem to provide a first ciphertext, and sending ~~a~~the first ciphertext to said remote party;

means for receiving a second ciphertext from said remote party~~,~~;

means for sending g^x modulo p to said remote party, and starting a clock;

means for receiving ~~a third ciphertext and~~ g^y modulo p from said remote party;

means for receiving a third ciphertext from said remote party, stopping the clock after receiving the third ciphertext, and computing an elapsed time interval of said clock;

means for deriving a key k_B from received g^y modulo p, ~~computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p~~, decrypting said second ciphertext with the key k_B to recover a second challenge signal from said remote ~~party,~~party;

means for computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p;

means for decrypting said third ciphertext with the key k_{AB} to recover a first response signal from said remote party;

means for verifying that said elapsed time of the clock is within a predetermined interval (TL_A, TU_A), where TL_A and TU_A are positive numbers;

means for verifying that said second challenge signal is produced by said remote party;

means for producing a second response signal of minimum duration T, encrypting said second response signal with the key k_{AB} to provide a fourth ciphertext and sending athe fourth ciphertext to said remote party;

means for verifying that said first response signal is a response produced by said remote party to said first challenge signal; and

means for ~~generating~~ using a key k from g^{xy} modulo p for secure communications with said remote party after verifying that said first response signal is a response produced by said remote party to said first challenge signal.

80. (Currently Amended) The apparatus according to claim 79, wherein said challenge signals and response signals represent biometrics characteristics ~~(such as voice signals)~~ of the ~~producing~~ authenticating and remote parties.

81. (Currently Amended) The apparatus according to claim 79, wherein verification of said first response signal and said second challenge signal from said remote party ~~is~~ are based on familiarity ~~of~~ with the remote party's biometrics characteristics. ~~Encryption of said challenge and response signals is performed using a cryptographic commitment function.~~

82. (Previously Presented) The apparatus according to claim 79, where TL_A is $t_1 + t_2$ and TU_A is $t_1 + t_2 + T$, with t_1 being the duration of said first challenge signal and t_2 being the duration of said first response signal.

83. (Currently Amended) A method of authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communication channel, said method including the steps of:

receiving a first ciphertext, containing a first challenge signal, from said remote party, generating a random number y, computing g^y modulo p, where g and p are numbers;

producing a ~~first~~ second challenge signal of minimum duration T, where T is a fixed time interval, and ~~it~~ is larger than the channel transmission and processing delay;

deriving a key k_B from g^y modulo p, encrypting said ~~first~~ second challenge signal with the key k_B and a symmetric key cryptosystem to provide a second ciphertext, and sending asaid second ciphertext to said remote party;

receiving g^x modulo p from said remote party, deriving a key k_A from g^x modulo p, decrypting said first ciphertext with the key k_A to recover ~~a~~ the ~~second~~ first challenge signal from said remote party;

verifying that said ~~second~~ first challenge signal is produced by said remote party, and producing a first response signal of minimum duration T;

computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, encrypting said first response signal with the key k_{AB} to provide a third ciphertext, and sending ~~a~~ the third ciphertext ~~and~~ to the remote party;

sending g^y modulo p to said remote party, and starting a clock;

receiving a fourth ciphertext, stopping the clock, and computing the elapsed time of the clock, and decrypting the fourth ciphertext with the key k_{AB} to recover a second response signal from said remote party;

verifying that said elapsed time of said clock is within a predetermined interval (TL_B, TU_B), where TL_B and TU_B are positive numbers;

verifying that said second response signal is a response produced by said remote party to said ~~first~~ second challenge signal; and

after verifying that said first challenge signal and that said second response signal are produced by said remote party and that said elapsed time is within the predetermined interval, ~~generating~~ using a key k from g^{xy} modulo p for secure communications with the remote party.

84. (Currently Amended) The method according to claim 83, wherein said challenge signals and response signals represent biometrics characteristics ~~(such as voice signals)~~ of the ~~producing~~ authenticating and remote parties.

85. (Currently Amended) The method according to claim 83, wherein verification of said ~~second~~ first challenge signal and said second response signal from said remote party ~~is~~ are based on familiarity ~~of~~ with the remote party's biometrics characteristics. ~~Encryption of said challenge and response signals is performed using a cryptographic commitment function.~~

86. (Currently Amended) The method according to claim 83, where TL_B is $t_3 + t_4$ and TU_B is $t_3 + t_4 + T$, with t_3 being the duration of the ~~first~~ second challenge signal and t_4 being the duration of the second response signal.

87. (Currently Amended) An apparatus for authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communication channel, said apparatus including:

means for receiving a first ciphertext, containing a first challenge signal, from said remote party, generating a random number y, computing g^y modulo p, where g and p are numbers;

means for producing a ~~first~~ second challenge signal of minimum duration T, where T is a fixed time interval and ~~it~~ is larger than the channel transmission and processing delay;

means for deriving a key k_B from g^y modulo p, encrypting said ~~first~~ second challenge signal with the key k_B and a symmetric key cryptosystem to provide a second ciphertext, and sending ~~a~~said second ciphertext to said remote party;

means for receiving g^x modulo p from said remote party, deriving a key k_A from g^x modulo p, decrypting said first ciphertext with the key k_A to recover ~~a second~~ the first challenge signal from said remote party;

means for verifying that said ~~second~~ first challenge signal is produced by said remote party, and producing a first response signal of minimum duration T;

means for computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, encrypting said first response signal with the key k_{AB} to provide a third ciphertext, and sending ~~a~~ the third ciphertext ~~and~~ to the remote party;

means for sending g^y modulo p to said remote party, and starting a clock;

means for receiving a fourth ciphertext, stopping the clock, and computing the elapsed time of the clock, and decrypting the fourth ciphertext with the key k_{AB} to recover a second response signal from said remote party;

means for verifying that said elapsed time of said clock is within a predetermined interval (TL_B, TU_B), where TL_B and TU_B are positive numbers;

means for verifying that said second response signal is a response produced by said remote party to said ~~first~~ second challenge signal; and

means for ~~generating~~ using a key k from g^{xy} modulo p for secure communications with the remote party, after verifying that said second response signal is a response produced by said remote party to said second challenge signal.

88. (Previously Presented) The apparatus according to claim 87, wherein said challenge signals and response signals are signals representing biometrics characteristics.

89. (Currently Amended) The apparatus according to claim 87, wherein verification of said ~~second~~ first challenge signal and said second response signal from the remote party ~~is~~ are based on familiarity ~~of~~ with the remote party's biometrics characteristics. ~~Encryption of said challenge and response signals is performed using a cryptographic commitment function.~~

90. (Currently Amended) The apparatus according to claim 87, where TL_B is $t_3 + t_4$ and TU_B is $t_3 + t_4 + T$, with t_3 being the duration of the ~~first~~ second challenge signal and t_4 being the duration of the second response signal.

91. (Currently Amended) A method of authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communication channel, said method including the steps of:

generating a first challenge signal of minimum duration T, where T is a fixed time interval, and ~~it~~ is larger than the channel transmission and processing delay;

generating a random number x, computing g^x modulo p, where g, and p are numbers, deriving a key k_A from g^x modulo p, encrypting said first challenge signal with the key k_A and a symmetric key cryptosystem to provide a first ciphertext, and sending ~~a~~ the first ciphertext to said remote party;

receiving a second ciphertext, sending g^x modulo p to said remote party, and starting a clock;

receiving g^y modulo p, computing a key k_B from g^y modulo p, decrytping the second ciphertext with the key k_B to recover a second challenge signal from said remote party;

verifying said second challenge ~~statement~~ signal to ensure that said second challenge ~~statement~~ signal is produced by said remote party, and producing a ~~first~~ second response signal of minimum duration T;

computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, encrypting said ~~first~~ second response signal with the key k_{AB} to provide a fourth ciphertext and sending ~~a~~ the ~~third~~ fourth ciphertext to said remote party;

receiving a ~~fourth~~ third ciphertext from said remote party, stopping said clock, decrypting the ~~fourth~~ third ciphertext with the key k_{AB} to recover a ~~second~~ first response signal from said remote party;

verifying that said elapsed time of said clock is within a predetermined interval (tl_A, tu_A), where tl_A and tu_A are positive numbers;

verifying that said ~~second~~ first response signal is a response produced by said remote party to said first challenge signal; and

after verifying that said second challenge signal and that said first response signal are produced by said remote party and that said elapsed time is within the predetermined interval, ~~generating~~ using a key k from g^{xy} modulo p for secure communications with said remote party.

92. (Previously Presented) The method according to claim 91, wherein said challenge signals and response signals are signals representing biometrics characteristics.

93. (Currently Amended) The method according to claim 91, wherein verification of said ~~second~~ first response signal and said second challenge signal from the remote party ~~is~~ are based on familiarity ~~of~~ with the remote party's biometrics characteristics. ~~Encryption of said challenge and response signals is performed using a cryptographic commitment function.~~

94. (Currently Amended) The method according to claim 91, where tl_A is $T_1 + T_2$ and tu_A is $T_1 + T_2 + T$, with T_1 being the duration of said first challenge signal and T_2 being the duration of said ~~second~~ first response signal.

95. (Currently Amended) An apparatus for authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communication channel, said apparatus including:

means for generating a first challenge signal of minimum duration T, where T is a fixed time interval, ~~and it~~ is larger than the channel transmission and processing delay;

means for generating a random number x, computing g^x modulo p, where g and p are numbers, deriving a key k_A from g^x modulo p, encrypting said first challenge signal with the k_A and a symmetric key cryptosystem to provide a first ciphertext, and sending ~~a~~ the first ciphertext to said remote party;

means for receiving a second ciphertext, sending g^x modulo p to said remote party, and starting a clock;

means for receiving g^y modulo p, computing a key k_B from g^y modulo p, decrytping the second ciphertext with the key k_B to recover a second challenge signal from said remote party;

means for verifying said second challenge ~~statement~~ signal to ensure that said second challenge ~~statement~~ signal is produced by said remote party, and producing a ~~first~~ second response signal of minimum duration T;

means for computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, encrypting said ~~first~~ second response signal with the key k_{AB} to provide a fourth ciphertext and sending ~~a third~~the fourth ciphertext to said remote party;

means for receiving a ~~fourth~~ third ciphertext from said remote party, stopping said clock, decrypting the ~~fourth~~ third ciphertext with the key k_{AB} to recover a ~~second~~ first response signal from said remote party;

means for verifying that said elapsed time of said clock is within a predetermined interval (tl_A, tu_A), where tl_A and tu_A are positive numbers;

verifying that said ~~second~~ first response signal is a response produced by said remote party to said first challenge signal; and

means for generating a key k from g^{xy} modulo p for secure communications with said remote party after verifying that said first response signal is a response produced by said remote party to said first challenge signal.

96. (Previously Presented) The apparatus according to claim 95, wherein said challenge signals and response signals are signals representing biometrics characteristics.

97. (Currently Amended) The apparatus according to claim 95, wherein verification of said ~~second~~ first response signal and said second challenge signal from the remote party ~~is~~ are based on familiarity ~~of~~ with the remote party's biometrics characteristics. ~~Encryption of said challenge and response signals is performed using a cryptographic commitment function.~~

98. (Currently Amended) The apparatus according to claim 95, where tl_A is $T_1 + T_2$ and tu_A is $T_1 + T_2 + T$, with T_1 being the duration of said first challenge signal and T_2 being the duration of said ~~second~~ first response signal.

99. (Currently Amended) A method of authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communication channel, said method including the steps of:

receiving a first ciphertext, containing a first challenge signal, from the remote party, generating a random number y, computing g^y modulo p, where g and p are numbers;

producing a ~~first~~ second challenge signal of minimum duration T, where T is a fixed time interval, and ~~it~~ is larger than the channel transmission and processing delay;

deriving a key k_B from g^y modulo p, encrypting said ~~first~~ second challenge signal with the key k_B and a symmetric key cryptosystem to provide a second ciphertext, and sending a second ciphertext to the remote party;

receiving g^x modulo p, computing a key k_A from g^x modulo p, decrypting said first ciphertext with the key k_A to recover ~~a second~~ the first challenge signal from remote party, sending g^y modulo p to the remote party and starting a clock;

verifying said ~~second~~ first challenge ~~statement~~ signal to make sure that said ~~second~~ first challenge ~~statement~~ signal is produced by said remote party, and then producing a first response signal of minimum duration T;

computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, encrypting said first response signal with the key k_{AB} to provide a third ciphertext and sending ~~a~~ the third ciphertext to said remote party;

receiving a fourth ciphertext from said remote party, stopping the clock, decrypting said fourth ciphertext with the key k_{AB} to recover a second response signal from said remote party;

verifying that said elapsed time of the clock is within a predetermined interval (tl_B, tu_B), where tl_B and tu_B are positive numbers;

verifying that said second response signal is a response produced by said remote party to said ~~first~~ second challenge signal; and

after verifying that said first challenge signal and that said second response signal are produced by said remote party and that said elapsed time is within the predetermined interval, ~~generating~~ using a key k from g^{xy} modulo p for secure communications with the remote party.

100. (Previously Presented) The method according to claim 99, wherein said challenge signals and response signals are signals representing biometrics characteristics.

101. (Currently Amended) The method according to claim 99, wherein verification of said ~~second~~ first challenge signal and said second response signal from said remote party ~~is~~ are based on familiarity ~~of~~ with the remote party's biometrics characteristics. ~~Encryption of said challenge and response signals is performed using a cryptographic commitment function.~~

102. (Currently Amended) The method according to claim 99, where tl_B is $T_3 + T_4$ and tu_B is $T_3 + T_4 + T$, with T_3 being the duration of said ~~first~~ second challenge signal and T_4 being the duration of said second response signal.

103. (Currently Amended) An apparatus for authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communication channel, said apparatus including:

means for receiving ~~a~~ first ciphertext, containing a first challenge signal, from the remote party, generating a random number y, computing g^y modulo p, where g and p are numbers;

means for producing a ~~first~~ second challenge signal of minimum duration T, where T is a fixed time interval, and ~~it~~ is larger than the channel transmission and processing delay;

means for deriving a key k_B from g^y modulo p, encrypting said ~~first~~ second challenge signal with the key k_B and a symmetric key cryptosystem to provide a second ciphertext, and sending ~~a~~ the second ciphertext;

means for receiving g^x modulo p, computing a key k_A from g^x modulo p, decrypting said first ciphertext with the key k_A to recover ~~a~~ the ~~second~~ first challenge signal from the remote party, sending g^y modulo p to the remote party and starting a clock;

means for verifying said ~~second~~ first challenge ~~statement~~ signal to make sure that said ~~second~~ first challenge ~~statement~~ signal is produced by said remote party, and then producing a first response signal of minimum duration T;

means for computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, encrypting said first response signal with the key k_{AB} to provide a third ciphertext and sending ~~a~~ the third ciphertext to said remote party;

means for receiving a fourth ciphertext from said remote party, stopping the clock, decrypting said fourth ciphertext with the key k_{AB} to recover a second response signal from said remote party;

means for verifying that said elapsed time of the clock is within a predetermined interval (tl_B, tu_B), where tl_B and tu_B are positive numbers;

means for verifying that said second response signal is a response produced by said remote party to said ~~first~~ second challenge signal; and

means for ~~generating~~ using a key k from g^{xy} modulo p for secure communications with the remote party, after verifying that said second response signal is a response produced by said remote party to said second challenge signal.

104. (Previously Presented) The apparatus according to claim 103, wherein said challenge signals and response signals are signals representing biometrics characteristics.

105. (Currently Amended) The apparatus according to claim 103, wherein verification of said ~~second~~ first challenge signal and said second response signal from said remote party ~~is~~ are based on familiarity ~~of~~ with the remote party's biometrics characteristics. ~~Encryption of said challenge and response signals is performed using a cryptographic commitment function.~~

106. (Currently Amended) The method according to claim 103, where tl_B is $T_3 + T_4$ and tu_B is $T_3 + T_4 + T$, with T_3 being the duration of said ~~first~~ second challenge signal and T_4 being the duration of said second response signal.

107. (New) The method according to claim 75, wherein the third ciphertext is received with g^y modulo p from said remote party and before the fourth ciphertext is sent.

108. (New) The method according to claim 75, wherein the fourth ciphertext is sent before the third ciphertext is received.

109. (New) The method according to claim 75, wherein said challenge signals and response signals comprise voice signals of the authenticating and remote parties.

110. (New) The method according to claim 75, wherein said challenge signals contain a freshness element, being an element indicative of when the challenge signal is generated.

111. (New) The method according to claim 75, further comprising, at the remote party:

receiving the first ciphertext, containing the first challenge signal, generating a random number y, computing g^y modulo p, where g and p are numbers;

producing the second challenge signal of minimum duration T, where T is a fixed time interval and is larger than the channel transmission and processing delay;

deriving a key k_B from g^y modulo p, encrypting said second challenge signal with the key k_B and a symmetric key cryptosystem to provide the second ciphertext, and sending said second ciphertext;

receiving g^x modulo p, deriving a key k_A from g^x modulo p, decrypting said first ciphertext with the key k_A to recover the first challenge signal;

verifying that said first challenge signal is produced by the party which provided the first ciphertext, and producing the first response signal of minimum duration T;

computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, encrypting said first response signal with the key k_{AB} to provide the third ciphertext and sending the third ciphertext;

sending g^{y} modulo p and starting a second clock;

receiving the fourth ciphertext, stopping the second clock, and computing the elapsed time of the second clock, and decrypting the fourth ciphertext with the key k_{AB} to recover the second response signal;

verifying that said elapsed time of said second clock is within a predetermined interval (TL_B, TU_B), where TL_B and TU_B are positive numbers;

verifying that said second response signal is a response produced by the party which provided the first ciphertext to said second challenge signal; and

after verifying that said first challenge signal and that said second response signal are produced by the party which provided the first ciphertext and that said elapsed time is within the predetermined interval, using a key k from g^{xy} modulo p for secure communications with the party which provided the first ciphertext.

112. (New) The apparatus according to claim 79, wherein

the means for receiving the third ciphertext further comprises the means for receiving g^{y} modulo p and is operable to receive the third ciphertext with g^{y} modulo p from said remote party; and

the means for receiving the third ciphertext is operable to receive the third ciphertext before the fourth ciphertext is sent.

113. (New) The apparatus according to claim 79, wherein the means for producing the second response signal is operable to send the fourth ciphertext before the third ciphertext is received.

114. (New) The apparatus according to claim 79, wherein said challenge signals and response signals comprise voice signals of the authenticating and remote parties.

115. (New) The apparatus according to claim 79, wherein said challenge signals contain a freshness element, being an element indicative of when the challenge signal is generated.

116. (New) The method according to claim 83, wherein g^y modulo p is sent to said remote party with the third ciphertext and before the fourth ciphertext is received.

117. (New) The method according to claim 83, wherein g^y modulo p is sent to said remote party after receiving g^x modulo p from said remote party and before the third ciphertext is sent.

118. (New) The method according to claim 83, wherein said challenge signals and response signals comprise voice signals of the authenticating and remote parties.

119. (New) The method according to claim 83, wherein said challenge signals contain a freshness element, being an element indicative of when the challenge signal is generated.

120. (New) The apparatus according to claim 87, wherein

the means for computing g^{xy} modulo p further comprises the means for sending g^y modulo p and is operable to send g^y modulo p to the remote party with the third ciphertext; and

the means for sending g^y modulo p is operable to send g^y modulo p to said remote party before the fourth ciphertext is received.

121. (New) The apparatus according to claim 87, wherein the means for sending g^y modulo p is operable to send g^y modulo p to said remote party after g^x modulo p is received from said remote party and before the third ciphertext is sent.

122. (New) The apparatus according to claim 87, wherein said challenge signals and response signals represent biometrics characteristics.

123. (New) The apparatus according to claim 87, wherein said challenge signals and response signals comprise voice signals of the authenticating and remote parties.

124. (New) The apparatus according to claim 87, wherein said challenge signals contain a freshness element, being an element indicative of when the challenge signal is generated.